ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024
No. 24-1113 (and consolidated cases)

IN THE
United States Court of Appeals
for the District of Columbia Circuit

TIKTOK INC. and BYTEDANCE LTD.
Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,
Respondent.

---

caption continued on inside cover

On Petitions for Review of Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act

---

SUPPLEMENTAL APPENDIX TO REPLY BRIEF OF PETITIONERS TIKTOK INC. AND BYTEDANCE LTD.

Andrew J. Pincus
Avi M. Kupfer
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3220
apincus@mayerbrown.com

Counsel for Petitioners TikTok Inc. and ByteDance Ltd.
(continued on inside cover)

Alexander A. Berengaut
Counsel of Record
David M. Zionts
Megan A. Crowley
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
aberengaut@cov.com

BRIAN FIREBAUGH et al.,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

BASED Politics Inc.,

Petitioner,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

John E. Hall
Anders Linderot
S. Conrad Scott
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, New York 10018
(212) 841-1000

Counsel for Petitioners TikTok Inc. and ByteDance Ltd.

TABLE OF CONTENTS*

* For ease of reference, this Supplemental Appendix is paginated consecutively from the end of Petitioners' original Appendix.

Presidential Documents

Memorandum of July 24, 2024

Delegation of Authority Under the Protecting Americans From Foreign Adversary Controlled Applications Act

Memorandum for the Secretary of State[,] the Secretary of the Treasury[,] the Secretary of Defense[,] the Attorney General[,] the Secretary of Commerce[,] the Secretary of Homeland Security[, and] the Director of National Intelligence

By the authority vested in me as President by the Constitution and the laws of the United States of America, including section 301 of title 3, United States Code, I hereby order as follows:

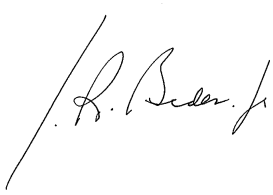
Section 1. (a) I hereby delegate to the Attorney General, in consultation with the Secretary of the Treasury, the Secretary of Commerce, and the Secretary of Homeland Security, all authorities vested in the President by the Protecting Americans from Foreign Adversary Controlled Applications Act (Division H of Public Law 118–50).

(b) In exercising the authorities delegated in subsection (a) of this section, the Attorney General may, as appropriate, consult with the Director of National Intelligence and the heads of other relevant executive departments and agencies (agencies).

Sec. 2. (a) There is established a Committee for the Review of Foreign Adversary Controlled Applications (Committee), composed of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence. Not later than 180 days after the date of this memorandum, the members of the Committee, through a process convened by National Security Council staff consistent with National Security Memorandum 2 of February 4, 2021 (Renewing the National Security Council System), shall determine rules and procedures sufficient for the Committee to exercise the authorities delegated to the Attorney General under section 1 of this memorandum. Upon conclusion of the 180-day period, the Committee shall exercise those authorities in accordance with such rules and procedures.

(b) The Director of National Intelligence and the heads of other relevant agencies, as the Attorney General under section 1 of this memorandum or the Committee under section 2 of this memorandum determines appropriate, shall provide assessments of the threat to national security posed by foreign adversary controlled applications in connection with the discharge of the responsibilities, respectively, of the Attorney General or the Committee. In providing such assessments, the Director of National Intelligence shall solicit and incorporate the views of the Intelligence Community, as appropriate.

Sec. 3. The Attorney General is authorized and directed to publish this memorandum in the *Federal Register*.



THE WHITE HOUSE,
Washington, July 24, 2024

[FR Doc. 2024–16741
Filed 7–26–24; 8:45 am]
Billing code 4410–19–P

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

TIKTOK INC., and BYTEDANCE LTD., *Petitioners*,	)	
v.	)	No. 24-1113
MERRICK B. GARLAND, in his official Capacity as United States Attorney General, *Respondent*.	)	

REPLY DECLARATION OF CHRISTOPHER P. SIMKINS

I, Christopher P. Simkins, under penalty of perjury, hereby declare as follows:

1. Through counsel for Petitioners TikTok Inc. and ByteDance Ltd. ("Petitioners"),[1] I have been asked to submit this Reply Declaration in response to specific points raised in three redacted declarations submitted by Respondent: Declaration of Casey Blackburn, Assistant Director of National Intelligence ("Blackburn Declaration"); Declaration of Kevin Vorndran, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation ("Vorndran Declaration"); and Declaration of David Newman, Principal Deputy Assistant Attorney General, National Security Division, Department of Justice ("Newman Declaration"). I will use the same definitions in this Reply Declaration as in my original Declaration filed on behalf of Petitioners.

[1] References to ByteDance are to the corporate group as opposed to any particular corporate entity. However, such references exclude TikTok U.S. Data Security Inc. ("TTUSDS").

2. Respondent's three Declarations collectively seek to make the case that the national security risk to the United States from the operation of TikTok, while under the ownership and control of ByteDance, cannot be mitigated by adoption and implementation of the NSA. They make a variety of statements regarding the threat and vulnerability posed by Petitioners and the TikTok U.S. App and TikTok U.S. Platform, and they assert that the NSA is insufficient in multiple respects. I will respond to their most salient arguments below.

3. At the outset, I reiterate my professional opinion that, if implemented as written, the NSA would effectively mitigate the U.S. national security risks identified by the government to be associated with ByteDance owning and deploying the TikTok U.S. App and the TikTok U.S. Platform. Respondent's Declarations do not change that opinion.

4. I start by offering two caveats to the views I express in this Reply Declaration. First, as noted in my first declaration, I assume for purposes of my declaration that the threat level associated with Petitioners TikTok Inc. and ByteDance Ltd. is HIGH. I understand Petitioners disagree with this assumption, and the analysis of this question is not within the scope of my first Declaration or this Reply Declaration. Rather, my focus is solely on whether, taking that threat level as a given, the NSA effectively mitigates the overall risk. Second, Respondent's Declarations contain classified information that has been redacted. I have not been given access to the classified version of the Declarations. My opinion is based solely on the public version of the Declarations as well as the record available to me, including the record provided to CFIUS in its investigation of Petitioners.

5. I have organized this Reply Declaration to respond to specific assertions in the Respondent's Declarations as to why the NSA cannot mitigate the national security risks

associated with the TikTok U.S. App and TikTok U.S. Platform. I address these assertions below. I have grouped them into the following categories:

- THREATS POSED BY CHINA AND CHINESE-OWNED COMPANIES (paras. 6-7)
- CONTROL OF THE RECOMMENDATION ENGINE (paras. 8-13)
- ACCESS TO PROTECTED DATA (paras. 14-23)
- DIFFICULTIES WITH SOURCE CODE REVIEW (paras. 24-35)
- INABILITY TO DETECT EXPLOITATION (paras. 36-38)
- INSUFFICIENT INDEPENDENCE OF TTUSDS (paras. 39-49)
- INABILITY TO MONITOR AND ENFORCE THE NSA (paras. 50-53)
- INADEQUACY OF THE "KILL SWITCH" (paras. 54-57)

THREATS POSED BY CHINA AND CHINESE-OWNED COMPANIES

6. Respondent's Declarations repeatedly make the point that the PRC's interests may be adverse to U.S. national security interests and that the PRC has the ability to directly or indirectly require Chinese-owned companies and their U.S. subsidiaries to support the Chinese strategic initiatives, even if doing so is contrary to the companies' commercial interests. For example, the Blackburn Declaration asserts that the "PRC may coerce ByteDance or TikTok to covertly manipulate the information received by the millions of Americans that use the TikTok application every day… in ways that benefit the PRC and harm the United States."[2] It further states that the "PRC has undertaken, undertakes, and will undertake overt and covert actions to undermine U.S. interests, public and private."[3] The Vorndran Declaration asserts that the PRC can "exert[] control over Chinese parent companies through formal legal means and, more

[2] Blackburn Decl. ¶ 9.

[3] Blackburn Decl. ¶ 23.

frequently, the informal business culture that surrounds the PRC's legal framework" and through that control can "access information from and about U.S. subsidiaries and compel their cooperation with PRC directives."[4]

7. As noted above and in my first declaration, I take these assertions regarding PRC intentions as a given and assume that the PRC poses a threat to U.S. national security, including through direct and indirect control of companies with operations in China or Chinese ownership. However, it would be an analytic mistake to use the existence of such a threat as a reason to conclude that the NSA is insufficient to mitigate the risk. The purpose of the analysis here is to ask whether the NSA is effective even if this threat is assumed. For such a threat to be actualized, it would require the PRC (or hypothetically the Petitioners) to take action to exploit the TikTok U.S. App and the TikTok U.S. Platform, which then begs the question of *how* that exploitation would occur. For purposes of the analysis, it is not relevant whether that exploitation has occurred in the past or is even occurring now. Instead, the analysis must focus on whether exploitation would be possible if the NSA were fully implemented. As I explained in my opening Declaration and will further reiterate in this Reply Declaration, my opinion is that the NSA effectively cuts off the avenues by which the types of exploitation animating the U.S. Government's concerns could occur. In other words, the security provisions in the NSA would make such exploitation sufficiently difficult or would limit the potential scope of exploitation sufficient to effectively mitigate the risks identified by the U.S. Government. Moreover, the NSA gives the U.S. Government and trusted U.S. third parties more visibility into the operations of TikTok than is possible for any other major social media network operating in the U.S., which itself is a boon to U.S. national security interests.

[4] Vorndran Decl. ¶ 10.

CONTROL OF THE RECOMMENDATION ENGINE

8. One of the key concerns raised by Respondent's Declarants is the potential for the PRC, via the TikTok U.S. Platform, to "covertly manipulate the information received by the millions of Americans that use the TikTok application every day… in ways that benefit the PRC and harm the United States."[5] The Blackburn Declaration asserts that "the content recommendation algorithm at the core of the TikTok application—and thus TikTok's success—resides within China and is largely maintained and controlled by ByteDance. This fact alone provides ByteDance with extremely powerful leverage over TikTok US."[6] The Vorndran Declaration likewise asserts that "the PRC could use its AI capabilities to augment its influence campaigns, such as amplifying preexisting social divisions, and targeting U.S. audiences through TikTok's algorithm by promoting and suppressing particular videos. The FBI assesses that this would occur covertly, with little, if any, outward sign of PRC control."[7]

9. Again, assuming for purposes of this declaration that the Declarant's concerns regarding propaganda and PRC influence in the U.S. are legitimate, the Declarants fail to address or even acknowledge the controls in the NSA around the Recommendation Engine. Put differently, the Declarants' ultimate risk assessment does not incorporate the protections and controls of the NSA. These controls are tailored specifically to address these concerns. First, the NSA requires that the Recommendation Engine be deployed in and operate from the Secure Oracle Cloud.[8] The training of the Recommendation Engine will take place in the United States

[5] Blackburn Decl. ¶ 9.
[6] Blackburn Decl. ¶ 76.
[7] Vorndran Decl. ¶ 32.
[8] *See* NSA Secs. 1.34, 8.4.

within the Secure Oracle Cloud and be controlled by TTUSDS.[9] Once the Recommendation Engine is deployed in the Secure Oracle Cloud, TTUSDS is required to observe and control the Recommendation Engine completely independently from ByteDance and TikTok US. TTUSDS and Oracle also audit the Recommendation Engine, and the promotion of content outside the Recommendation Engine, to ensure that it conforms to the published policies for the TikTok U.S. App.[10] In short, TTUSDS and Oracle—not ByteDance and TikTok US—will be in control of the Recommendation Engine and its operations in the United States.

10. Second, the NSA contains provisions regarding Source Code review by TTUSDS, Oracle, and the Source Code Inspector to ensure that there is nothing malicious in any Source Code provided by ByteDance.[11] This specifically includes Source Code for the Recommendation Engine.[12] The purpose of this Source Code review with respect to the Recommendation Engine is not necessarily to inspect how the recommendation algorithm makes decisions, which I understand is largely driven by content and user behavior, but to prevent a third party (including Petitioners) from covertly manipulating the Recommendation Engine once it is deployed by TTUSDS and Oracle in the Secure Oracle Cloud.

11. TTUSDS's oversight of the Recommendation Engine and Content Promotion and Filtering, as well as control over their deployment, will include the participation of a Content Advisory Council of external social media, free speech, and content moderation experts who are resident U.S. citizens.[13] This Council will be appointed by and answerable to TTUSDS, not

[9] *See* NSA Sec. 9.13(2)(i).
[10] *See* NSA Secs. 2.4(5), 9.13(2).
[11] *See* NSA Secs. 2.4, 9.5-9.13, 9.15.
[12] *See* NSA Secs. 1.28, 9.7, 9.13.
[13] *See* NSA Secs. 5.4, 9.13(1).

ByteDance or TikTok US. The Council will review the "playbook" that is created by Petitioners that describes the procedures and rules for human-aided content moderation.[14] A copy of the "playbook" will also be given to the U.S. Government and Oracle.[15]

12. The concerns that the PRC or ByteDance can feed data into the Recommendation Engine to subtly guide it to carry out propaganda is belied by the fact that they will not have sufficient technical access to feed the Engine with data. Under the terms of the NSA, "any data that is collected on U.S. user interaction with content on the TikTok U.S. Platform as an input into the Recommendation Engine" is "Protected Data" that will be stored and managed by TTUSDS and Oracle within the Secure Oracle Cloud.[16] TTUSDS, not ByteDance or TikTok US, will control operation and deployment of the Recommendation Engine for the TikTok U.S. Platform and the TikTok U.S. App.

13. Given this level of rigor and the controls that will be placed in the hands of U.S. persons at TTUSDS and Oracle, as well as the visibility to the U.S. Government via monitoring and compliance, it is difficult to give credence to generalized assertions that the PRC and ByteDance will somehow continue to be able to influence and manipulate the Recommendation Engine. The reality is that, in light of the controls created by the NSA, PRC interests likely will have more ability to influence other social media platforms that operate in the U.S. than it will the TikTok U.S. Platform that is protected in the Secure Oracle Cloud.

[14] *See id.*

[15] *See* NSA Sec. 9.13(1).

[16] *See* NSA Sec. 1.22.

ACCESS TO PROTECTED DATA

14. The Vorndran Declaration states that "[t]he FBI assesses ByteDance and TikTok could facilitate the PRC's access to U.S. users' data, which could enable PRC espionage, technology transfer, data collection, and influence activities."[17] The Newman Declaration acknowledges that the NSA contains provisions seeking to prevent Petitioners from having access to Protected Data, but then argues that "the proposed role for Oracle under ByteDance's proposal would not have resolved the Executive Branch's national security concerns because, among other things, the proposed agreement contemplated extensive data flows of U.S. users back to ByteDance and thus to China."[18]

15. The Newman Declaration makes three principal assertions to support this proposition. First, the Newman Declaration asserts that Oracle "would be faced with the challenge of the massive scale of data that could be transported back to Beijing for ostensibly legitimate purposes. [Oracle] would be required to sift through such data, using both untested and experimental tools to try to ascertain whether information was routed for legitimate commercial reasons or nefarious reasons at the request of PRC actors."[19] The Newman Declaration further asserts that Oracle would not be able to adequately identify and secure the Protected Data because it will have to "rely on precision in source code review and access controls that were by definition incomplete, with significant volumes of excepted information able to travel to the PRC for engineering and commercial reasons."[20] The Newman Declaration expands on this concern, stating "[t]he treatment of Excepted Data represented a large loophole

[17] Vorndran Decl. ¶ 18.
[18] Newman Decl. ¶ 6.
[19] Newman Decl. ¶ 85.a.
[20] Newman Decl. ¶ 81.

in the Final Proposed NSA's data protection regime. Users could opt into their data being treated as Excepted, placing U.S. national security interests in private hands."[21]

16. To begin with, this is a mischaracterization of the basic thrust of the NSA and is premised on a mistaken notion about the volume of data flow. The NSA specifically prohibits the flow of Protected Data to China, including any "anonymized" data.[22] The NSA provisions outline some categories of data that can be sent to ByteDance, but those exceptions are narrow, and subject to the explicit consent of the U.S. Government. It is not correct, as the Newman Declaration asserts, that any user can "opt-in" to having their data treated as excepted.[23] Further, the NSA requires TTUSDS and Oracle to monitor and if necessary to "block" any unexpected or unauthorized network connectivity or traffic between the TikTok U.S. App or TikTok U.S. Platform and any platform operated by ByteDance, with the decision to block being in the "sole discretion" of Oracle.[24]

17. The concern also does not take account of the capabilities of Oracle, which is a sophisticated and highly capable U.S. technology company with decades of experience managing complex datasets and a long-standing customer relationship with the U.S. Government.[25] It would be surprising to say the least for Oracle to enter into agreements to deliver these controls, which would be highly visible to the U.S. Government, if Oracle felt incapable of delivering.

---

[21] Newman Decl. ¶ 109.

[22] *See* NSA Secs. 1.22, 9.8, 11.7-11.9, 11.12.

[23] *See* NSA Secs. 1.11, 1.23, 11.1-2.

[24] *See* NSA Sec. 9.17(1).

[25] *See e.g., Defense and Intelligence*, Oracle (last accessed Aug. 6, 2024), https://perma.cc/PD4X-WNW3.

And none of Respondent's Declarations identify any particular reason why Oracle would lack the expertise or resources to handle its assigned tasks.

18. Finally, the concern that Oracle would have to rely solely on Source Code review misunderstands the function of a mitigation agreement in this context. Oracle would most certainly not be relying on Source Code review alone to monitor the flow of Protected Data. In fact, network configuration, access controls, authorization requirements, and monitoring and logging of data traffic will play as much or more into securing Protected Data as review of the Source Code. Information security specialists within TTUSDS and Oracle would have controls in place to manage these configurations and could ensure that only authorized personnel have credentials to key systems and applications.[26]

19. Second, the Newman Declaration asserts that the NSA was "designed so that ByteDance and its engineers would continue to have access to data for some purposes and would continue to be involved in engineering, source code and algorithm development, code testing, and user testing. [Oracle] and other independent monitors and auditors would have theoretically been able to see that data left the U.S. storage regime to go back to ByteDance, but those independent monitors and auditors would have no way (that the Executive Branch is aware of) to be able to distinguish legitimate transfers of U.S. person data from nefarious transfers of U.S. person data."[27]

20. The NSA prohibits Petitioners from possessing or having access to Protected Data, in connection with Source Code development or otherwise.[28] The generalized assertion in

[26] See NSA Secs. 9.8, 9.17.
[27] Newman Decl. ¶ 85.b.
[28] *See* NSA Secs. 1.22, 9.8, 11.5.

the Newman Declaration that broad swaths of user data will be made available to ByteDance developers is accordingly simply not true. The NSA does allow for TTUSDS and Oracle to send "Excepted Data" to ByteDance.[29] This category of Excepted Data does not include "anonymized" user data—such anonymized user data must remain Protected Data.[30] The NSA states expressly that "TTUSDS shall ensure that Excepted Data does not contain any Protected Data…before transmitting any Excepted Data to ByteDance."[31]

21. The NSA contemplates that some data related to user identifiers such as usernames or phone numbers may be needed solely for the purpose of routing TikTok traffic to the TikTok U.S. Platform, and can accordingly be included within Excepted Data, but even this limited set of data must be "hashed."[32] A "hash" is a one-way cryptographic function that obfuscates the underlying data by using a cryptographic key to translate data into integer values. In my professional roles, including as DOJ's representative on CFIUS, as a technology consultant to corporations across the United States (including some of the world's leading cybersecurity companies), and as the co-founder and CEO of my own cybersecurity company, I have decades of experience with structuring data protection protocols. I have often designed security protocols to use hashing functions to protect sensitive data. In my experience, trying to reverse a hashing function to discover the underlying data (in the absence of having access to the key) is exceptionally difficult. Hashing is often used by the U.S. Government to protect sensitive

[29] *See* NSA Sec. 11.1(2).

[30] *See* NSA Secs. 1.11, 1.22, 11.1. The category of Excepted Data does include a defined list, subject to U.S. Government approval, of aggregated/averaged business metrics data with no association with any kind of identity or user information (and even anonymized identifiers removed).

[31] NSA Sec. 11.1(2).

[32] *See* NSA Sec. 1.11(4).

data. Even at the nation-state level, efforts to reverse hashed data through brute force methods is limited to rare circumstances involving only the highest priority national security missions. The Newman Declaration does not address the security implications of hashing the relevant data.

22. Finally, the Newman Declaration notes that the NSA allows Protected Data to flow to ByteDance and TikTok US pursuant to "Limited Access Protocols" and then asserts that these protocols would give ByteDance "access to data in a wide range of scenarios," such as "validating user regions for proper routing, threats of harm to employees, bots and other malicious accounts associated with hate groups, foreign influence campaigns, transnational organized crime, international fraud, emergency responses including terrorism, suicide attempts by a user, and for legal scenarios including eDiscovery, litigation, regulatory responses, and compliance investigations."[33] Without explaining why, the Newman Declaration states that under these Limited Access Protocols, "ensuring that Protected Data w[as] accessed only for legitimate ends[] would have been impossible."[34]

23. This concern about Limited Access Protocols is at odds with the terms of the NSA. To begin with, the NSA authorizes TTUSDS, not ByteDance or TikTok US, to be the principal entity for following Limited Access Protocols, including responding to law enforcement requests.[35] The NSA does allow for Protocols to be established where the Petitioners could have access to Protected Data for the following specific reasons: "legal and compliance matters and certain other emergency situations involving the health, safety, and security of TikTok users and the public in and outside the United States."[36] However, the

[33] Newman Decl. ¶ 107.
[34] Newman Decl. ¶ 108.
[35] *See* NSA Sec. 7.1
[36] NSA Sec. 11.9.

Protocols themselves, which will establish the specific ground rules and use cases under which TTUSDS will release Protected Data (i.e., Petitioners will not be able to "pull" or "gather" the Protected Data, but instead will be given data if the Protocols are met), must be written out and presented to the U.S. Government for approval, with U.S. government having discretion regarding such approvals and any conditions required for the approvals.[37] Far from being a broad flow of data that would be impossible to monitor, the Limited Access Protocols would govern discrete releases of data by trusted parties (TTUSDS and Oracle) according to rules approved by the U.S. Government. The Newman Declaration again does not address these procedures.

DIFFICULTIES WITH SOURCE CODE REVIEW

24. Respondent's Declarants seek to cast doubt on the effectiveness of Source Code review as a part of the NSA's security measures. They assert that Chinese law will not allow Petitioners to export the Source Code.[38] To the extent Respondent's Declarants are concerned that Petitioners would not provide Source Code for review under the NSA because PRC approval is required and would be withheld, this would clearly constitute a material breach of the NSA by Petitioners, triggering all of the remedies available to the U.S. Government under the NSA, including the suspension of user access to the TikTok U.S. Platform.[39]

25. The Declarants correctly point out that ByteDance will continue to develop Source Code that will be reviewed and deployed in the United States by TTUSDS and Oracle, although they mistakenly assert that ByteDance will "deploy[]" the Source Code.[40] The NSA is

[37] See NSA Sec. 11.9(2).
[38] *See* Blackburn Decl. ¶¶ 76, 78.
[39] *See* NSA Secs. 21.2, 21.3(6), 21.4.
[40] *See* Newman Decl. ¶¶ 15, 99.c.

very clear that only TTUSDS and Oracle will deploy the Source Code (once it is built into binary code) from the Secure Oracle Cloud, with Petitioners having no role in that deployment.[41]

26. Setting aside this threshold factual error, the Newman Declaration contains several assertions about the difficulties of Source Code review that are contrary to the NSA or are not consistent with the practical realities of Source Code review. First, the Declaration asserts that the size of the Source Code is too large to be effectively reviewed by Oracle: "Though varying over time, ByteDance's representations as to the size of the TikTok platform's Source Code leave no doubt that a complete review of each line would be a monumental undertaking. Most recently, ByteDance represented to the Executive Branch in 2022 that the Source Code contained 2 billion lines of code. For comparison, the Zoom application contains 10 million lines of code, and Windows Operating System contains approximately 50 million. Even if static, Oracle estimated it would require three years to review this body of code. But the Source Code is not static; ByteDance regularly updates it to add and modify TikTok's features. Even with Oracle's considerable resources, perfect review would be an impossibility."[42]

27. First, this size comparison is misleading and is an "apples to oranges" comparison. The intent appears to be to suggest the size of the code base inherently makes source code review an unachievable task. However, the referenced statistics for Windows and Zoom are for software *applications*, not platforms that operate both on local devices and on remote servers. The size estimate given by the Newman Declaration is for the entirety of the

[41] *See* NSA Secs. 8.4, 9.12.

[42] *See* Newman Decl. ¶ 80.

TikTok U.S. Platform and the TikTok U.S. App combined.[43] Different components of the TikTok platform such as the TikTok U.S. App, on their own, represent a fraction of the 2 billion lines based on my review of the record presented to CFIUS. According to information provided by Petitioners to CFIUS in 2022, for example, the TikTok U.S. App on iOS devices contained 18.6 million lines of code.

28. More importantly, the size of the code base is not the principal consideration when considering the efficacy of Source Code review. In my various professional roles, I have had substantial experience with using Source Code review as a tool in constructing holistic, overarching security programs. As a member of CFIUS, and in conjunction with government agencies such as FBI and NSA, I personally structured code review programs for systems and networks that were at least as large as the TikTok U.S. App and the TikTok U.S. Platform. They included code review for not just platforms but also network infrastructure such as telecommunications equipment, mobile wireless infrastructure, and biometric identity platforms. I have also instituted programs for Source Code review within some of the largest global cybersecurity providers that protect U.S. Government components. In my experience, the complexity in Source Code review is less about the size of the code base and more about how the code is structured, the amount of open-source code included, and the code configurations that are inherent in its architecture. Mr. Newman's apparent belief that source code review was impracticable in the case of TikTok simply because the size of the code base ignores these considerations.

[43] As a size comparison, public reports from nearly 10 years ago suggest that at the time Google was 2 billion lines of code. *See* Cade Metz, *Google is 2 Billion Lines of Code-And It's All in One Place*, Wired (Sep. 16, 2015), https://perma.cc/V875-2S6F.

29. The NSA includes a commitment on the part of Oracle to finishing the initial Source Code review within 180 days of execution of the NSA.[44] This is a scalable task because industry-standard code review today typically involves a mix of automated scans, comparisons of open-source libraries that have been copied into the code base (i.e., comparing them against the publicly available libraries to see discrepancies), and manual review of discrete portions of the code.[45] Source code review under the NSA will be further facilitated by the requirement in the NSA that Petitioners provide Oracle a software bill of materials identifying all code modules that are embedded in the Source Code, which essentially functions as a map.[46] Once an initial base review of the Source Code is completed, revisions and updates are compared against original reviewed code to understand differences. Moreover, part of Source Code review will also include running binary (built) Code in secure environments to test behavior and functions.[47] The NSA requires that there be a full history of reviewed Code so that if anomalies arise, there is a way to show when and where they showed up in the Code base.[48] Again, the Newman Declaration fails to address any of these approaches—which include industry-standard techniques for source code review—in reaching his conclusion that Source Code review is not feasible because of the size of the codebase.

---

[44] *See* NSA Sec. 9.9(1).

[45] *See, e.g.*, *Source Code Security Analyzers*, National Institute of Standards and Technology (last updated Feb. 12, 2024), https://perma.cc/DB2S-H9ZD; Ibrahim Haddad, *Open Source Guides: Using Open Source Code*, The Linux Foundation (last accessed Aug. 12, 2024), https://perma.cc/SBF6-HLA7.

[46] *See* NSA Sec. 9.2

[47] *See* NSA Secs. 8.4, 9.12(4)-(5).

[48] *See* NSA Sec. 9.12(1).

30. In addition to reviewing all Code for both the TikTok U.S. App and the TikTok U.S. Platform, including the Recommendation Engine,[49] TTUSDS and Oracle will have sole and complete control over how it is deployed and what network connections and access will be allowed because the Code must be deployed in the Secure Oracle Cloud.[50]

31. On top of all of that, yet another third party—the Source Code Inspector—must review the entirety of the Source Code process and ensure that TTUSDS and Oracle have complied with best practices and their security obligations under the NSA.[51] The engagement of the Source Code Inspector is subject to the U.S. Government's approval (through non-objection).[52] If the U.S. Government is not satisfied with any aspect of the Source Code review process, it can request at any time and in its sole discretion additional security testing of the Source Code using any other generally accepted practices to ensure the security of both the Source Code and Executable Code.[53]

32. Taking all of that together, it is difficult to imagine a more robust Source Code review process than that which is included in the NSA. The Newman Declaration fails to take account of these provisions in concluding that Source Code review was an insurmountable task.

33. The Newman Declaration next asserts that even if Source Code review is effective, it will not be enough to prevent the PRC or Petitioners from subverting national security: "Even assuming every line of Source Code could be monitored and verified by [Oracle], the PRC could exert malign influence through the very same features that have made

[49] *See* NSA Sec. 9.10.
[50] *See* NSA Secs. 8.4, 9.12.
[51] *See* NSA Sec. 9.11.
[52] *See id.*
[53] *See* NSA Sec. 9.14.

the TikTok platform globally successful. For example, the TikTok platform includes a feature known as 'heating,' by which employees may manually boost certain content for viewing on users' For You Pages. Users cannot see that a video has been 'heated' when they view it. Heating is useful from a commercial perspective, as it enables TikTok to curate popular content and disseminate that content widely on the platform, potentially increasing user engagement and increasing the value of advertising it sells. But it may also be used to drive views of content of the PRC's choosing. A review of the Source Code, in other words, would not and could not satisfy that the platform's features would be used for benign commercial ends, not malicious ones, thus inhibiting the government from detecting noncompliance with the Final Proposed NSA."[54]

34. This assertion represents a misunderstanding of how the NSA deals with "heating," which is a part of the Content Promotion and Filtering function described in the NSA.[55] The Newman Declaration suggests that a human sitting within ByteDance will be able to use access to the TikTok U.S. Platform—specifically software that is used for Content Promotion and Filtering—to manually suggest propaganda in favor of the PRC. The reality is that any "heating" or "filtering" (i.e., removing or demoting content, rather than promoting it) of content by Petitioners for the TikTok U.S. Platform would be implemented through TikTok USDS, subject to the protections of the NSA, and highly auditable and monitorable. Under the NSA, such "heating" or "filtering" would be considered Content Promotion and Filtering.[56]

[54] Newman Decl. ¶ 78.b.
[55] *See* NSA Secs. 1.6, 9.13.
[56] See NSA Sec. 1.6.

Under the NSA, TTUSDS, with support from Oracle, will be responsible for auditing Content Promotion and Filtering in the United States.[57]

35. Based on the information presented to CFIUS, any video campaign selected for "heating" is assigned a Program ID. TTUSDS will be responsible for approving and deploying that Program ID and the associated Software before allowing videos associated with that campaign to be promoted to U.S. users.[58] In addition, Oracle and the Third-Party Monitor would review the Content Promotion and Filtering software and data for compliance with relevant policies.[59] If there is any "material inconsistenc[y]" between the Source Code or the data and the policies, Oracle and the Third-Party Monitor will be required to report their findings to the Board of TTUSDS.[60] The TTUSDS Board, Oracle, and the U.S. government can also each call for an audit of these processes at any time by the Third-Party Auditor.[61] In short, the so-called "heating" is not an avenue for circumvention, but instead is a process that will be heavily scrutinized and monitored under the NSA. Further, the entire process involves a series of auditable activities that can be readily verified.

INABILITY TO DETECT EXPLOITATION

36. The Newman Declaration makes several statements that together assert it will be too difficult for TTUSDS and Oracle or the U.S. Government to detect exploitation by Petitioners, even if the NSA is faithfully implemented.[62] For example, the Newman Declaration suggests that the Petitioners and ostensibly other Chinese-controlled companies might gather

[57] *See* NSA Sec. 2.4(4).
[58] See NSA Sec. 9.13.
[59] See *id.*
[60] *See* NSA Sec. 9.13(2).
[61] *See id.*
[62] *See, e.g.,* Newman Decl. ¶ 76.

data flowing from U.S. users to other locations around the world: "The flow of U.S. user data into TTUSDS's servers, and from there to other locations, would not be subject to direct U.S. government monitoring under the Final Proposed NSA."[63] As mentioned above, the Newman Declaration also includes "heating" as a purported method of evading the NSA. The suggestion is that neither TTUSDS nor Oracle could monitor these avenues of exploitation.

37. As discussed above, it is factually incorrect to assert that "heating" will be an effective way to avoid detection under the NSA. TTUSDS will be responsible for approving and deploying a promotion campaign's assigned Program ID and the associated Software before allowing videos associated with that campaign to be promoted to U.S. users.[64] As noted above, TTUSDS will control the deployment of Content Moderation and Filtering in the Oracle Cloud. Moreover, the process generates highly auditable artifacts, and Oracle and the Third-Party Monitor will review those artifacts against the written policies for Content Promotion and Filtering.[65]

38. Regarding the purported flow of data outside the United States, this is a misunderstanding of how the TikTok U.S. App and the TikTok U.S. Platform work. The inference being made is that the U.S. Government would be unable to monitor flows of data in and out of the Oracle cloud. But the NSA requires TikTok USDS and Oracle to identify and monitor all interactions and data elements, including all user data, between the TikTok U.S. App

[63] *See, e.g.,* Newman Decl. ¶ 78.a.
[64] See NSA Sec. 9.13.
[65] See NSA Sec. 9.13(2).

and the TikTok U.S. Platform, on the one hand, and any other internet host, on the other hand.[66] And Oracle is required to block any unexpected or unauthorized flows of data.[67]

INSUFFICIENT INDEPENDENCE OF TTUSDS

39. For the NSA to be effective, TTUSDS must have sufficient independence from ByteDance and TikTok US to effectively implement the NSA without the threat of PRC control or influence. The Newman Declaration acknowledges that the Board of TTUSDS "would consist of three directors, none with ByteDance or TikTok US. affiliations, to be approved by the Executive Branch, with ostensibly no duty to report to TikTok US. or to ByteDance."[68] However, the Newman Declaration cites several examples that it argues cast doubt on whether these governance provisions will be effective. The Newman Declaration concludes that "[a]lthough the Final Proposed NSA had not been signed, and therefore ByteDance was under no obligation to the U.S. government to guarantee TTUSDS's operational independence, … the Executive Branch … doubt[ed] the true independence TTUSDS would possess under the Final Proposed NSA, if enacted."[69]

40. The Newman Declaration's discussion on the Executive Branch's lack of trust in ByteDance and the insufficient operational independence of TTUSDS does not support this conclusion.

41. First, the Newman Declaration asserts that the corporate governance model for TTUSDS's independence will not be sufficient because the U.S. Government cannot trust the

[66] *See* NSA Sec. 9.17.
[67] *See id.*
[68] Newman Decl. ¶ 52.
[69] Newman Decl. ¶ 99.

Petitioners' and TTUSDS's motivations for complying with the NSA.[70] By way of background, the governance provisions in the NSA for TTUSDS (i.e., the reliance on independent Outside Directors) are modeled on governance provisions that have been used by the U.S. Government in hundreds of mitigation agreements. CFIUS adopted these corporate governance provisions from the Defense Department, which uses them to give U.S. subsidiaries of a foreign parent sufficient independence from the foreign ownership, control, and influence ("FOCI") of their foreign parent(s) when performing classified work for the U.S. Government.

42. These FOCI governance provisions require the U.S. subsidiary to have a Board of Directors that includes "Outside Directors" or "Proxy Holders," who are U.S. citizens with no prior affiliation with the foreign parent and are approved by the U.S. Government.[71] Under the NSA, the term "Security Directors" is used instead of "Outside Directors."[72] These Board structures are placed between the protected U.S. subsidiary and all of the corporate parent(s) above it, including between other U.S. corporations in the ownership chain. The NSA actually goes farther than the typical FOCI case where foreign parents are allowed to have at least one "Inside Director" on the Board. The NSA requires the TTUSDS Board be comprised of *only* Security Directors.[73] These Security Directors that govern and control TTUSDS owe a fiduciary duty to the U.S. Government, not ByteDance or TikTok US.[74]

---

[70] *See* Newman Decl. ¶¶ 95, 99.

[71] *See Foreign Ownership, Control or Influence*, Defense Counterintelligence and Security Agency (last visited Aug. 12, 2024), https://perma.cc/J7JQ-D8WD.

[72] *See* NSA Sec 3.1.

[73] *See* NSA Sec. 3.1(1). Typically, the U.S. subsidiary's Board must also include one or more "Inside Directors," who are representatives of the foreign parent and are not required to be U.S. persons.

[74] *See* NSA Sec. 3.6.

43. In asserting that the U.S. Government cannot trust TTUSDS's independence, the Newman Declaration claims that U.S. Government agencies, including the Defense Department, will only entertain this corporate governance mitigation mechanism "with companies it assesses are motivated to comply solely by business incentives: retaining their U.S. Government contracts in order to maximize profits. For these businesses, maximizing profit is their primary motivation, and failure to comply with a FOCI mitigation agreement exposes them to losing significant profits from classified contracts. On the other hand, for companies that are controlled by a hostile foreign power seeking to penetrate the United States, national objectives may outweigh business incentives. This is true even for otherwise legitimate companies."[75] The inference is that the Petitioners and TTUSDS cannot be trusted because they could be forced to comply with PRC directives that are contrary to their economic missions.

44. This critique in the Newman Declaration misses a critical aspect of the NSA: the role for Oracle as the trusted third party responsible for implementing the most significant mitigation measures. Even if the U.S. Government believes it cannot trust the Petitioners to truly give TTUSDS its independence, the Newman Declaration fails to explain why the U.S. Government cannot rely on Oracle to faithfully implement the NSA.

45. In any event, it is inaccurate to say that DOD, CFIUS, and other U.S. Government agencies will only entertain the use of these corporate governance mechanisms when the foreign parent company can be counted on to be motivated solely by economic incentives such as maintaining government contracts. The U.S. Government has relied on corporate governance measures for FOCI mitigation in scores of situations where there was negative intelligence reporting about the intentions of foreign parent companies, as well as in situations where the

[75] Newman Decl. ¶ 89.

home country of the foreign parent was known to have interests that are contrary to U.S. national security interests. Therefore, these arguments cannot be used to suggest that the NSA will fail to give TTUSDS sufficient independence.

46. The Newman Declaration next seeks to cast doubt on TTUSDS independence by focusing on governance over TikTok US as a whole, as opposed to TTUSDS. The Newman Declaration cites a number of ways in which ByteDance will continue to have the ability to interact with and influence the TikTok US Board. For example, "ByteDance would still be an essential member for any quorum of the TikTok US Board, have rights to be a member of all committees designated by the TikTok US Board, and have to vote in the affirmative for TikTok to take certain actions."[76] Based on this, the Newman Declaration concludes that "[o]nly a divestment can wholly eliminate ByteDance and TikTok's presence and capability to wield influence on the U.S. companies' boards of directors."[77]

47. First, this mischaracterizes the TikTok US Board under the NSA. Specifically, under the NSA, the TTUSDS chair is the only director specifically required for a quorum of the TikTok US Board and any committee thereof. Additionally, while decisions of the TikTok US Board would generally require an affirmative vote by a majority of the directors in office, of which at least 2 of at least 5 would be employees of ByteDance or its affiliates, the only director that would "have to vote in the affirmative for TikTok to take certain actions" is the TTUSDS chair as it relates to certain "matters dealing with the relationship with or responsibilities of

[76] Newman Decl. ¶ 94; *see also id.* ¶ 95.d.

[77] Newman Decl. ¶ 94.

[Oracle]" or "issues that directly impact [ByteDance and TikTok US's] compliance with" the NSA.[78]

48. More fundamentally, this discussion of ByteDance's participation at the TikTok US level misses the primary point of the NSA's provisions regarding independence. While the NSA does include some controls at the TikTok US level, as discussed above, the primary purpose of the NSA is to give TTUSDS—not TikTok US—independence from both ByteDance and TikTok US. All critical security provisions and operational control of the TikTok App and TikTok Platform in the United States would be controlled by TTUSDS, not TikTok US.[79]

49. Finally, the Newman Declaration includes several asserted anecdotes regarding the Petitioners' behavior. The Newman Declaration relies on these anecdotes to establish that despite the FOCI corporate governance mitigation measures in the NSA, TTUSDS will not in fact remain independent from ByteDance and TikTok US. These anecdotes do not support the Newman Declaration's conclusions:

A. For example, one anecdote relates to a story published by Forbes suggesting that ByteDance is still today playing a role in TTUSDS operations: "Moreover, the audio recordings of ByteDance meetings obtained by Forbes indicate that ByteDance retained considerable control and influence over TTUSDS operations."[80] However, this argument is belied by the fact that the NSA has never been signed and the FOCI mitigation contemplated therein is not yet fully implemented. The Newman Declaration acknowledges this point: "ByteDance

[78] *See* NSA Sec. 4.3.
[79] *See* NSA Sec. 2.4.
[80] Newman Decl. ¶ 95.a.

has voluntarily implemented some components of the Final Proposed NSA, although the agreement was never signed."[81]

B. The Newman Declaration also argues that Petitioners "communicated to the Executive Branch that they envisioned frequent meetings between TTUSDS and TikTok US to ensure TTUSDS's continued alignment with the global TikTok platform."[82] This is actually precisely in line with how FOCI governance mitigation mechanisms work, both in the CFIUS and the Defense Department FOCI contexts. In virtually every such context, protected U.S. subsidiaries are authorized to interact with foreign-owned parent companies to coordinate on business matters. The NSA specifically contemplates this.[83] The whole point of having Security Directors with fiduciary obligations to protect U.S. national security is to monitor and control if, when, and how interactions take place between the foreign parent and the protected U.S. subsidiary.

C. Finally, the Newman Declaration asserts that TTUSDS would not be independent as a result of the use by TTUSDS of an internal communication application developed by ByteDance called "Lark": "Despite the Final Proposed NSA's contemplation of U.S. Government approval for TTUSDS's choices of vendors, negotiators for ByteDance expressed ByteDance's intention that employees of TTUSDS would continue to use certain ByteDance products, such as Lark (a ByteDance proprietary platform for in-office communications), which collected

[81] Newman Decl. ¶ 50, fn. 6.

[82] Newman Decl. ¶ 96.

[83] *See* NSA Sec. 4.2.

and stored large amounts of personal data."[84] First, Newman ignores the fact that under the NSA, use by TTUSDS of Lark or any other software would be subject to the same restrictions on the storage of and access to Protected Data that apply generally.[85] Second, there is nothing in the record to indicate that the U.S. Government ever asked that the NSA be modified to forbid the use of such internal tools as a general matter. Third, as discussed in more detail below, the NSA requires that TTUSDS's operations be audited and monitored by multiple third parties.[86] If any one of those monitors or auditors believed Lark posed a security vulnerability, they could alert the Security Directors as well as the U.S. Government and require a change. This is part of the purpose of having independent governance at the Board level—TTUSDS would be able to make its own decision whether to use Lark or any other application, regardless of the opinion or intention of Petitioners.

INABILITY TO MONITOR AND ENFORCE THE NSA

50. In conjunction with the assertion discussed above that TTUSDS will not be sufficiently independent, the Newman Declaration suggests that the U.S. Government will be left with having to trust Petitioners to faithfully implement the NSA. The Declaration asserts that such trust will not be possible: "Most fundamentally, the Final Proposed NSA … still permitted ByteDance executives to exert leadership control and direction over TikTok's US operations, and still contemplated extensive contacts between the executives responsible for the TikTok U.S.

[84] Newman Decl. ¶ 97.

[85] *See* NSA Secs. 11.5, 11.8.

[86] *See* NSA Secs. 14.1-14.6, 15.1, 16.1-16.6.

platform and ByteDance leadership overseas. Moreover, the Final Proposed NSA would ultimately have relied on the Executive Branch trusting ByteDance to make day-to-day business decisions that enforce the mitigation measures even as the Executive Branch lacked the resources and capabilities to fully monitor and verify ByteDance's compliance with the Final Proposed NSA."[87]

51. The Newman Declaration then asserts that in the absence of such trust, the U.S. Government will be left to rely on robust monitoring and enforcement and that there simply are not enough resources available to do this effectively: "[T]he Executive Branch lack[s] the resources and capabilities to fully monitor and verify ByteDance's compliance with the Final Proposed NSA"[88] The Declaration attributes this to the "size and technical complexity of the TikTok platform and its underlying software"[89] and the "massive data flows between the United States and the PRC and the opacity of TikTok's algorithm,"[90] as well as an assertion that "TikTok's legitimate and … illegitimate activities are externally indistinguishable."[91] The Vorndran Declaration also asserts that the U.S. Government—specifically the FBI—lacks both the expertise and resources to assist with monitoring.[92]

52. These assertions about the lack of U.S. Government resources ignore the fact that the primary burden of monitoring compliance with the NSA does not fall on the U.S.

---

[87] Newman Decl. ¶ 75.

[88] Newman Decl. ¶ 75.

[89] Newman Decl. ¶ 79.

[90] Newman Decl. ¶ 115.b.ii.

[91] Newman Decl. ¶ 115.b.ii.

[92] Vorndran Decl. ¶¶ 36, 46 ("The FBI does not independently monitor compliance with CFIUS NSAs. It does not have agents or analysts devoted to monitoring these agreements and instead would only get involved when one of the co-lead agencies seeks FBI review.").

Government. Instead, it falls to a series of U.S. third party entities that are contractually charged with ensuring that TTUSDS and Oracle are discharging their responsibilities under the NSA. These entities must be approved by CFIUS and owe fiduciary obligations to CFIUS for reporting security violations. All of these will be funded by Petitioners, not the U.S. Government.[93] They include not only the Trusted Technology Provider (Oracle), but also the Source Code Inspector discussed above, as well as a Third-Party Monitor (conducts ongoing oversight of the actual implementation of the NSA and a principal point of contact for the U.S. Government regarding compliance),[94] a Third-Party Auditor (conducts an independent audit of compliance by Petitioners and TTUSDS upon request by the U.S. Government),[95] and a Cybersecurity Auditor (conducts technical audits of TTUSDS's and Oracle's compliance, including with implementation of Source Code review, deployment of the Platform in the Secure Oracle Cloud, and the storage and protection of Protected Data).[96]

53. By design, these third parties have the technical and operational expertise to ensure effective monitoring within their respective areas of focus and, under the NSA, generally have reporting obligations directly to the U.S. Government.[97] Rather than being required to deploy its own agents and analysts to conduct monitoring, the U.S. Government will review the findings and submissions of these third parties and make decisions about what actions to take, if any, including enforcement and penalties. The U.S. Government plays this exact role of reviewing third party monitoring and auditing in scores of CFIUS contexts where parties have

[93] *See* NSA Secs. 8.2(7), 9.11(1), 14.6, 15.1, 16.4(12).
[94] *See* NSA Secs. 16.1-16.6.
[95] *See* NSA Sec. 15.1.
[96] *See* NSA Secs. 14.1-14.6.
[97] *See* NSA Secs. 9.11(2), 14.3, 15.1, 16.4(2).

been required to enter into mitigation agreements to protect national security. The Newman and Vorndran Declarations do not explain why U.S. Government resource constraints undermine the efficacy of the NSA given the multiple layers of third-party monitoring that will be funded by Petitioners, not the U.S. Government.

INADEQUACY OF THE "KILL SWITCH"

54. The Newman Declaration asserts that the so-called "kill switch" remedy in the NSA, whereby the U.S. Government could stop the operation of the TikTok U.S. App and the TikTok U.S. Platform in the U.S., is ineffective and is not a "realistic option to deter noncompliance with the Final Proposed NSA."[98] The Declaration makes several statements as to why the kill switch remedy could not be used effectively.

55. First, the Declaration states that "its use would have required the government to know, in sufficient time to act, of an imminent threat" and that the purported lack of ability to monitor the NSA (as discussed above) would diminish the ability to know of such imminent threat.[99] As discussed above, however, the Declaration here again ignores a key line of defense in the NSA, which is Oracle. Oracle is required to operate the TikTok U.S. App in accordance with the Security Protocols, and TTUSDS and Oracle are generally responsible for the security of the TikTok U.S. Platform.[100] Oracle is also responsible for securing the access to Protected Data and ensuring that the Recommendation Engine is operating exclusively in its own Secure Oracle Cloud.[101] If Oracle or any other trusted party under the NSA (each of which serve as additional lines of defense), such as TTUSDS or the Third-Party Monitor, discovers a violation,

[98] Newman Decl. ¶ 111. Petitioners alternatively refer to this remedy as a "shut-down option."
[99] Newman Decl. ¶ 111.
[100] *See* NSA Secs. 2.4, 9.8.
[101] *See* NSA Secs. 8.4, 9.12-13, 11.5.

they have a duty to report concerns immediately. The NSA provides that "any actual or potential violation of this Agreement" must be reported to the appropriate Technology Officer, the Third-Party Monitor, and the U.S. Government "as soon as practicable, but in any event within one (1) day of learning of the actual or potential violation."[102]

56. Second, the Newman Declaration asserts that the kill switch remedy is not effective because it would allow for only a "temporary stop" for only a "specific list of narrowly scoped NSA violations," with most of those violations being obvious breaches of the NSA.[103] The Declaration asserts that the "temporary stop would not, however, give the U.S. Government anything resembling complete discretion to shut down the TikTok platform based on its own independent assessment of national security risk and assessments from the U.S. Intelligence Community. For example, the provision does not permit a temporary stop based on concerns related to the algorithm or whether U.S. persons' data is accessible by the PRC government."[104]

57. The Newman Declaration's characterization of the kill switch remedy is inaccurate in several respects. For one thing, as the Newman Declaration itself recognizes elsewhere, the kill switch remedy is available for concerns related to the algorithm (it applies to deployment of unreviewed source code) and to concerns about access to U.S. users data (it applies to Protected Data access controls).[105] It also ignores a separate provision of the NSA that allows Oracle to suspend user access to the TikTok U.S. Platform specifically where Oracle identifies issues related to the Source Code, with the suspension continuing until Oracle in its

[102] NSA Sec. 10.6.
[103] Newman Decl. ¶ 114.b.
[104] Newman Decl. ¶ 114.c.
[105] NSA Sec. 21.3(7), (10).

sole discretion is satisfied that ByteDance modifies the Source Code to remedy those issues.[106] Further, there is nothing in the NSA to indicate that the U.S. Government must wait to be told by the Petitioners or even Oracle that a problem has arisen. The NSA is very clear that the determination of whether the Petitioners have violated the NSA is solely within the U.S. Government's sole discretion: "The CMAs, in their sole discretion, may determine whether a violation has occurred, if such violation warrants the imposition of a Penalty or further action, and the appropriate Penalty amount or action, if any."[107] And if the U.S. Government determines there is a violation, it can trigger the temporary stop, which must become effective within three days.[108] As with any mitigation agreement entered into by the U.S. Government, there is always a possibility of litigation. But, the NSA specifically authorizes the U.S. Government to "seek any and all remedies available under applicable law, including injunctive or other judicial relief."[109] The NSA states that if the Petitioners do not comply with a temporary stop order, the U.S. Government "may direct" Oracle to suspend "user access to the TikTok U.S. Platform."[110] I am personally unaware of any other unilateral remedy of this magnitude in a CFIUS mitigation agreement. Mitigation agreements entered into by the Defense Department to protect classified information do not contain unilateral remedies of this sort.

CONCLUSION

58. After reviewing Respondent's Declarations, my assessment is that the Declarations—and the Newman Declaration in particular—misunderstand or disregard important

[106] NSA Sec. 9.15(2).
[107] NSA Sec. 21.1.
[108] NSA Sec. 21.3.
[109] NSA Sec. 21.2.
[110] NSA Sec. 21.5.

provisions of the NSA, leading to inaccurate conclusions about the NSA and how it will be implemented. The Newman Declaration also makes technical and operational assumptions that fail to address current industry practices and standards.

59. Having carefully considered Respondent's Declarations, my professional opinion remains unchanged—if implemented as written, the NSA would effectively mitigate the U.S. national security risks associated with Petitioners owning and deploying the TikTok U.S. App and the TikTok U.S. Platform.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this day August 14, 2024.

Christopher P. Simkins

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

TIKTOK INC. and BYTEDANCE LTD., *Petitioners*, v. MERRICK B. GARLAND, in his official capacity as Attorney General of the United States, *Respondent*.	)	No. 24-1113

REPLY DECLARATION OF STEVEN WEBER

I, Steven Weber, under penalty of perjury, hereby declare as follows:

1. I am a Professor of the Graduate School at the University of California, Berkeley ("UC Berkeley"), where I hold joint appointments as Professor of the School of Information and in the Department of Political Science. I am also a Partner at Breakwater Strategy, a strategic insights and communications firm. I have been retained by counsel for Petitioners TikTok Inc. and ByteDance Ltd. (the "Petitioners") in this action to analyze certain reported justifications for the Protecting Americans from Foreign Adversary Controlled Applications Act (the "Act").

2. I submitted a declaration in this case on June 20, 2024 that analyzed two reported justifications for the Act: (1) the security of the data that TikTok collects from its U.S. users, particularly as it relates to alleged risks of disclosure to the Chinese government; and (2) the possibility that TikTok's recommendation algorithm could be misused for the benefit of the Chinese government, either by censoring certain content or promoting propaganda or disinformation. In my first declaration, I explained, among other things, that (i) the concerns that reportedly animated the Act "are issues that the industry confronts as a whole and are not unique or distinctive to TikTok," (ii) "TikTok's approach for dealing with these issues is in line with—and in many respects markedly better than—industry best practices," and (iii) based on my experience and expertise, "there is no evident national security rationale for the Act's particular focus on TikTok."[1] A copy of my declaration is available at pages 760 to 798 of Petitioners' appendix.

3. Since submitting my first declaration, I have reviewed the materials that the government publicly filed on July 26, 2024, July 30, 2024, and August 9, 2024 in defense of the

[1] App'x to Br. of Petitioners at 762, 788, *TikTok, Inc. v. Garland*, No. 24-1113 (D.C. Cir. June 20, 2024), ECF No. 2060757 ("Pet'rs App'x).

Act, including redacted versions of the government's brief and appendix.[2] Nothing in those filings alters the assessment I provided in my first declaration. I submit this supplemental declaration solely to address certain specific points raised in the government's public filings. The fact that I am not addressing a claim made by the government should not be interpreted to mean that I agree with it.

I. Data Security

4. The government's brief states that TikTok collects "vast amounts of personal information" about its users, which the government claims "can be used for all sorts of intelligence operations or influence operations."[3] The government's brief and supporting declarations focus on two types of "personal information" purportedly collected by TikTok: (i) U.S. users' "precise locations," and (ii) "contact lists" stored in U.S. users' phones.[4] While the government acknowledges that TikTok collects and uses these categories of information for "legitimate business purposes," including "suggesting contacts to follow" and "targeting advertisements" to U.S. users, the government contends that such information "can be used to harm the United States' national security."[5] The government's statements about TikTok's data collection practices are inaccurate in several respects.

---

[2] Public Redacted Br. for Respondent, *TikTok, Inc. v. Garland*, No. 24-1113 (D.C. Cir. July 26, 2024), ECF No. 2066896; Public Redacted Gov't App'x, *TikTok, Inc. v. Garland*, No. 24-1113 (D.C. Cir. July 26, 2024), ECF No. 2066897 ("Gov't App'x"); Amended Public Redacted Br. for Respondent, *TikTok, Inc. v. Garland*, No. 24-1113 (D.C. Cir. July 30, 2024), ECF No. 2067517 ("Gov't Br."); Notice of Filing of Redacted Transcript, *TikTok, Inc. v. Garland*, No. 24-1113 (D.C. Cir. Aug. 9, 2024), ECF No. 2069332.

[3] Gov't Br. at 27–28.

[4] *Id.* at 8–9, 18, 27–28, 34; Gov't App'x at 35–37 (Vorndran Decl.).

[5] Gov't App'x at 35–37 (Vorndran Decl.).

5. First, I am not aware of any evidence that TikTok collects "precise location" data from U.S. users. In the technology industry, "precise location" data commonly refers to location data gathered using GPS technology, often in conjunction with WiFi, Bluetooth, and cellular data.[6] That is also how mobile device companies, like Apple and Google, use the term.[7] TikTok states in its Privacy Policy that current versions of the U.S. TikTok app do not collect GPS data from U.S. users and that no version of the app released after August 2020 has collected such data.[8] I am unaware of any evidence that contradicts this assertion. Nothing in the government's submission, for example, establishes or even asserts that current versions of the U.S. TikTok app collect GPS data from U.S. users. Accordingly, it is inaccurate to claim as the government does that TikTok collects "precise location" data from U.S. users, as that term is commonly used and defined in the technology industry.

6. To be sure, TikTok collects IP address and country information from U.S. users, which can be used to approximate users' geographic locations.[9] But IP addresses are a significantly less precise—and often inaccurate—way to attempt to identify a user's geographic location. While a GPS-enabled cell phone is capable under some conditions of accurately

[6] *See, e.g.*, Dan Komosny, Miroslav Voznak & Saeer Ur Rehman, *Location Accuracy of Commercial IP Address Geolocation Databases*, 46 J. of Info. Tech. 333, 334 (2017), https://perma.cc/Z5PK-SDWV (comparing IP geolocation to "GPS-precise locations"); Clare Stouffer, *What Is An IP Address? A Definition + How to Find It*, Norton (Nov. 20, 2023), https://perma.cc/KQN3-EP5C ("IP addresses do reveal your geolocation, but not your precise location like a home address does.").

[7] *See Turn Location Services and GPS On or Off on Your iPhone, iPad, or iPod Touch*, Apple (Mar. 26, 2024), https://perma.cc/A98Z-4QTN; *Manage Location Permissions for Apps*, Google Account Help, https://perma.cc/3W8T-FR7E.

[8] *Privacy Policy*, TikTok, https://perma.cc/2DW2-TPSP.

[9] *Id.*

identifying a user's location to within a five-meter radius,[10] IP-based geolocation provides only a rough estimate of a user's location (*e.g.*, to within multi-mile radius) and may be inaccurate for a variety of reasons. MaxMind, an IP intelligence firm that maintains a commercial IP geolocation database, has stated that its IP geolocation products are capable of estimating a device's location within the U.S., plus or minus 50 kilometers, between 77% and 81% of the time.[11] IP2Location, another company that maintains an IP geolocation database, has stated that its geolocation product correctly estimates a device's location within the U.S., plus or minus 50 miles, 76.32% of the time.[12] The accuracy and precision of estimating a *mobile* device's location based on IP address information is even lower. MaxMind, for instance, states that it can correctly estimate a mobile device's geographic location within the U.S., plus or minus 50 kilometers, between 38% and 42% of the time.[13] Because TikTok does not collect GPS information from U.S. users, I disagree with the government's assertion that TikTok "has access to the precise locations" of U.S. users.

7. Second, with respect to TikTok's ability to access users' contact list information, the government fails to mention that TikTok may access a user's contact list only if the user gives TikTok express permission to do so.[14] This is a common practice among applications. Indeed, a number of social media companies, including Instagram and X (formerly Twitter), collect users' contact lists to connect them to other app users whom the user already knows.[15]

---

[10] GPS Accuracy, GPS.gov, https://perma.cc/8U95-YRV6.

[11] *GeoIP2 City Accuracy*, MaxMind, https://perma.cc/T2VY-HFCP.

[12] *IP Geolocation Data Accuracy*, IP2Location, https://perma.cc/X6Z6-45JT.

[13] *GeoIP2 City Accuracy*, MaxMind, https://perma.cc/X3D8-GGM4.

[14] *Privacy Policy*, TikTok, https://perma.cc/2DW2-TPSP.

[15] *Privacy Policy: Friends, Followers and Other Connections*, Instagram, https://perma.cc/37RX-KG3C; *X Privacy Policy*, X (Sept. 29, 2023), https://perma.cc/6XST-39LA.

8. Finally, it bears mention that the government does not assert that TikTok collects data from U.S. users that is different in amount or kind than the data typically collected from U.S. users by other applications, including foreign-owned applications.[16] As I explained in my first declaration, "the type and amount of data that TikTok collects from U.S. users . . . is comparable to the type and amount of data that other social media platforms and applications collect from U.S. users."[17] The government does not appear to disagree.[18]

II. Content Recommendation

A. NCRI Study

9. In his declaration, Casey Blackburn, Assistant Director of National Intelligence, admits that he has "no information that the [People's Republic of China] has . . . coerce[d] ByteDance or TikTok to covertly manipulate the information received by . . . Americans that use the TikTok application . . . , through censorship or manipulation of TikTok's algorithm."[19] Mr. Blackburn's declaration is consistent with a number of studies that have analyzed the TikTok platform and similarly concluded that there is no evidence that TikTok is systematically promoting

[16] *See, e.g.*, *Privacy Policy*, Instagram, https://perma.cc/U9DF-9UG7; *X Privacy Policy*, X (Sept. 29, 2023), https://perma.cc/6XST-39LA; *Yelp Privacy Policy*, yelp (Jan. 1, 2023), https://perma.cc/JNJ4-L8AQ; *Shein Privacy Policy*, Shein (Mar. 11, 2024), https://perma.cc/X5YD-2M27; *Temu | Privacy Policy*, Temu (Mar. 30, 2024), https://perma.cc/6KGC-PK38; Nicholas Kaufman, *Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes*, U.S.-China Econ. & Security Review Comm'n (Apr. 14, 2023), https://perma.cc/LW3U-E65P.

[17] *See* Pet'rs App'x at 764–65 (Weber Decl.).

[18] The government also does not appear to disagree with my conclusion that there are a variety of ways that a nation-state actor, like China, may acquire information about U.S. citizens, including by purchasing "U.S. user data through the broader, multi-layered data brokerage market." *Id.* at 767–69. Nor does the government appear to disagree with my conclusion that many multinational companies, including U.S. companies, maintain ties with and/or have operations in China. *Id.* at 770–72.

[19] Gov't App'x at 4 (Blackburn Decl.).

pro-China and/or anti-U.S. content or censoring content that may be critical of China and/or sympathetic to the United States or its allies.[20]

10. Mr. Blackburn also cites a December 2023 study from the Network Contagion Research Institute (the "NCRI Study"), which he claims "underscores" the government's "concern" that China may attempt to censor or manipulate TikTok's algorithm in the future.[21] In the NCRI Study, researchers purported to compare the use of certain hashtags on TikTok to the use of the same hashtags on Instagram and found a lower incidence of TikTok posts related to topics adverse to China's national interests as compared to Instagram posts on the same topics.[22] From this, the researchers suggested that "[w]hether content is promoted or muted on TikTok appears to depend on whether it is aligned [with] or opposed to the interests of the Chinese Government."[23] In my analysis, the NCRI Study suffers from a number of methodological flaws that call its findings and conclusions into question.

11. As others have noted, the authors of the NCRI Study made two fundamental errors in designing the study and interpreting its results.[24] First, in designing the study, the researchers "failed to account for how long each platform has existed."[25] Instagram was launched in 2010 and

---

[20] Laura Edelson, *Getting to Know the TikTok Research API*, Cybersecurity for Democracy, https://perma.cc/V3AJ-8JEP; Milton L. Mueller & Karim Farhat, *TikTok and U.S. National Security*, Georgia Inst. of Tech. Internet Governance Project, at 12–13 (2023), https://perma.cc/JR3Z-F5TK.

[21] Gov't App'x at 21 (Blackburn Decl.).

[22] *A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives*, Network Contagion Research Institute (Dec. 2023), https://perma.cc/57L2-A9RW ("NCRI Study").

[23] *Id.* at 3.

[24] Paul Matzko, *Lies, Damned Lies, and Statistics: A Misleading Study Compares TikTok and Instagram*, CATO Institute (Jan. 2, 2024), https://perma.cc/ZZ5X-8TTE.

[25] *Id.*

is thus nearly twice as old as TikTok, which was launched internationally in 2017. Given the platforms' different launch dates, "topics that were the subject of intense public discourse in the early 2010s, but which have not been heavily featured in the decade since"—*e.g.*, activism related to Tibet—would be expected to be less well represented on TikTok over its lifespan than Instagram over its lifespan.[26]

12. Notably, the authors of the NCRI Study were *not* assessing posts uploaded to Instagram and TikTok during a discrete time period (*e.g.*, the last six months of 2023). Rather, the authors were assessing posts uploaded to the platforms over the *entirety* of the platforms' existence.[27] Given this design flaw, the researchers' failure to account for variations in the salience of political issues over time further undermines the conclusions they draw from their analysis.

13. Second, the authors of the NCRI Study failed to account for the fact that TikTok and Instagram have users of different age demographics, with TikTok users trending younger than those who use Instagram.[28] Because different age groups have different interests and viewpoints that might account for some of the observed variation in posts, the study's failure to attempt to correct for the age demographic characteristics of each platform's users "led them to miss the potential for generational cohort effects," once again weakening the validity of conclusions drawn from the study.[29]

14. The NCRI Study suffers from other methodological issues:

a. The researchers' decision to analyze the number of posts uploaded to each platform, as opposed to the number of views such posts receive, is an important flaw given

[26] *Id.*

[27] NCRI Study at 5.

[28] Matzko, *supra* note 24.

[29] *Id.*

the conclusions they purport to draw. As the researchers were attempting to assess whether TikTok is "promot[ing] or mut[ing]" content based on "whether it is aligned or opposed to the interests of the Chinese Government,"[30] information about the number of *views* that posts receive—as opposed to the number of posts themselves—would appear to be the more appropriate dependent variable, as viewership information more directly measures users' access to and engagement with content on a platform. Indeed, if a foreign government were aiming to influence public perceptions and opinions on a sensitive issue, they surely would be aiming for views not posts as the dependent variable to measure the success of their propaganda campaign. Screenshots published along with the NCRI Study show that the authors of the study had access to view counts associated with TikTok and Instagram posts, and so it is concerning that they declined to use that data.[31]

b. Apart from differences in the platforms' *age* demographics discussed above, the NCRI Study rests on the unsubstantiated assumption that the *geographic* demographics of Instagram and TikTok are the same. Because the researchers did not consider differences in the apps' popularity or availability around the world, they did not consider whether demographic differences might account for differences in hashtag data.

c. The NCRI Study uses global Instagram and TikTok data to draw conclusions about the experience of U.S. users on the app.[32] But there is no basis for the authors'

[30] NCRI Study at 3.

[31] *Id.* at 19–20.

[32] *Id.* at 5.

assumption that global hashtag data is similar to U.S. hashtag data. Because the researchers have not established that global hashtag data is consistent with U.S. hashtag data, the conclusions they draw about U.S. users' experiences on the apps are unsubstantiated.

d. The NCRI Study methodology is also susceptible to selection bias in the hashtags that were chosen. The authors of the NCRI study do not explain why they selected the particular hashtags they used, and whether they considered but rejected other hashtags that satisfied their stated criteria ("topics directly sensitive to the Chinese Government"),[33] but did not fit with their narrative. For example, the hashtag #spyballoon has a comparable number of posts on TikTok (8238) and Instagram (9767).

e. The authors of the NCRI Study assert that, after the release of the study, "TikTok removed the public hashtag search feature for analyzing trends on its platforms," which the authors surmise was meant "to deliberately obscure public access and transparency."[34] The authors of the NCRI study relied on a tool on the TikTok website intended for advertisers, and they do not mention that nearly a year before the study was published, TikTok launched a "Research API" to allow qualifying researchers "to study public data about TikTok content and accounts."[35] Contrary to the authors' assertion, TikTok's Research API—which remains available to

[33] *Id.* at 3.

[34] *Id.* at 18.

[35] *See Research Tools*, TikTok, https://perma.cc/2EG6-745Q; Mariella Moon, *TikTok Opens Data to US Researchers in Its Bid to Be More Transparent,* Engadget (Feb. 21, 2023), https://perma.cc/W584-RZ6D; Pet'rs App'x at 809 (Presser Decl.)

researchers today—includes a "public hashtag search feature." Indeed, other researchers have used this public hashtag search feature in their academic studies of TikTok.[36]

B. Heating

15. In its brief, the government states that "TikTok and ByteDance 'employees regularly engage' in a practice' called 'heating,' in which certain videos are manually promoted to 'achieve a certain number of video views.'"[37] The government further states that "TikTok does not disclose which posts are 'heated,' and public reporting found that China-based employees had 'abused heating privileges,' with the potential to dramatically affect how certain content is viewed."[38] The implication is that TikTok's practices with respect to heating are concerning or represent a departure from the practices of its peers in the industry.

16. The source the government identifies for these assertions about heating is a January 2023 *Forbes* article by Emily Baker-White, titled "TikTok's Secret 'Heating' Button Can Make Anyone Go Viral."[39] As an initial matter, this article does not support the statements made in the government's brief. For example, the article never states that "China-based employees . . . 'abused heating privileges.'"[40] While the article refers to certain instances in which "heating was used improperly by employees," the article does not assert that such employees were based in China or used heating to further China's national interests.[41] On the contrary, the instances of heating

[36] Edelson, *supra* note 20.

[37] Gov't Br. at 37.

[38] *Id.*

[39] *Id.* (quoting Emily Baker-White, *TikTok's Secret 'Heating' Button Can Make Anyone Go Viral*, Forbes (Jan. 20, 2023), https://perma.cc/GE2X-WW4B).

[40] Baker-White, *supra* note 39.

[41] *Id.*

misuse identified in the article concern incidents in which employees violated company policy by "heat[ing] their own accounts, as well as accounts of people with whom they have personal relationships."[42] As I noted in my first declaration, the risk that corporate insiders will engage in conduct that violates company policy is an industry-wide issue that affects nearly every company, both within and outside the technology industry.[43] In my assessment, the risk of employee misconduct as described in this article is not a basis for distinguishing TikTok from other platforms.

17. Nor is the fact that TikTok engages in heating in the first place a basis for the Act's differential treatment of TikTok. As the *Forbes* article acknowledges, all technology companies, including Google and Meta, "engage, in some degree, in efforts to amplify specific posts to their users."[44] For example, public reporting shows that Facebook prioritizes posts in users' newsfeeds that have "sparked lots of comments and replies" on the site, a strategy that Facebook believes increases users' engagement.[45] Platforms also regularly promote content on specified topics.[46]

18. In addition to promoting content themselves, platforms also enable promotion of content by users and others. X, for example, prioritizes the replies of users who pay to subscribe

[42] *Id.*

[43] Pet'rs App'x at 775–76 (Weber Decl.) (describing risks associated with "the potential access to, and misuse of, data by corporate insiders for purposes not authorized by company policy" and recounting instances of such misuse at Google, Meta, and Uber).

[44] Baker-White, *supra* note 39.

[45] Will Oremus, *et al.*, *How Facebook Shapes Your Feed*, Wash. Post (Oct. 26, 2021), https://perma.cc/8TA7-4STJ.

[46] *See, e.g.*, Laurie Richardson, *Our Ongoing Work to Support the 2022 U.S. Midterm Elections*, Google (Sept. 1, 2022), https://perma.cc/X9YQ-38X6 (describing Google's efforts to "connect voters with information about voter registration and how to vote"); *Promoting Authoritative Information about COVID-19 Vaccines*, Meta, https://perma.cc/NXL7-VVFS (describing Facebook's "campaign to promote authoritative information about COVID-19").

its "X Premium" service"[47] and allows users to pay to promote their own posts.[48] Foreign actors have utilized these types of features for improper ends. In the lead up to the 2016 election, Russia's Internet Research Agency created Facebook posts designed to "sow discord and polarize voters in the United States" and then used the social media company's advertising platform to promote those posts among certain demographics, including African Americans, Mexican Americans, and conservative voters.[49] Facebook estimated that 150 million Facebook and Instagram users were exposed to these posts in 2016.[50]

C. Acts of Alleged "Censorship" Outside of the United States

19. In its brief and supporting declarations, the government states that TikTok has engaged in "censorship" outside of the United States. For example, Mr. Vorndran refers to reporting about ByteDance purportedly censoring content for applications available in China in response to Chinese government demands.[51] "Censorship" is a loaded term, and it is not clear precisely what the government means to allege through this statement. To the extent the allegation is that TikTok has made editorial decisions outside of the United States in response to requests or demands from foreign governments, or to comply with foreign law, such an allegation (if true) would not be a basis for distinguishing TikTok from other U.S. companies. Indeed, many U.S.

---

[47] *About X Premium*, X Help Center, https://perma.cc/9544-K5EG.

[48] *How To Increase Your Reach*, X Help Center, https://perma.cc/Z47C-PX27.

[49] Kate Fazzini, *Here's How the Russians Targeted Social Media Posts to Influence the 2016 Election, According to a New Independent Report*, CNBC (Dec. 27, 2018), https://perma.cc/FF6H-282S.

[50] Cecilia Kang, Nicholas Fandos & Mike Isaac, *Russia-Financed Ad Linked Clinton and Satan*, N.Y. Times (Nov. 1, 2017), https://perma.cc/6HUZ-6QVR.

[51] Gov't App'x at 38. Mr. Newman's discussion of this same incident is misleading insofar as it suggests that censorship at China's behest occurred outside of China. *Id.* at 72–73. As Mr. Vorndran's declaration makes clear, the reporting on this incident related to services provided *within* China. *Id.* at 38.

companies engage in such activities. In 2023, for example, Twitter (now known as X) admitted that it restricted access to certain content in Turkey in advance of the country's presidential election in response to threats by the Turkish government to shut down the app in Turkey unless it removed such content from the platform.[52] In 2021, India introduced a set of "IT rules" that require, among other things, social media platforms to warn users "not to post anything that's defamatory, obscene, invasive of someone else's privacy, encouraging of gambling, harmful to a child or 'patently false or misleading.'"[53] The rules further require social media platforms to take down posts at the government's direction and, upon request, to identify the original source of offending information.[54] Public reporting indicates that a number of U.S. companies, including Google, Facebook, X, and LinkedIn, are complying with India's rules, "at least partially."[55]

20. Indeed, it is common for social media companies operating globally to state that they will comply with local laws in the jurisdictions in which they operate. Facebook, Instagram, X, and YouTube all include language to this effect on their websites,[56] and a number of

---

[52] Megan Cerullo, *Twitter Under Fire for Restricting Content Before Turkish Presidential Election*, CBS News (May 16, 2023), https://perma.cc/QV56-HFN5.

[53] Lauren Frayer & Shannon Bond, *India and Tech Companies Clash Over Censorship, Privacy and 'Digital Colonialism'*, NPR (June 10, 2021), https://perma.cc/2UR9-6EXX.

[54] *Id.*

[55] *Id.*; Varsha Bansal, *India's Government Wants Total Control of the Internet*, WIRED (Feb. 13, 2023), https://perma.cc/VL3P-HH9B; Surabhi Agarwal, *Facebook Says It Aims To 'Comply' With India's New IT Rules Effective Tomorrow*, Economic Times (May 25, 2021), https://perma.cc/LJE6-DFYA.

[56] *Content Restrictions Based on Local Laws: H2 2023 Report*, Meta, https://perma.cc/TZJ9-U4TP ("When something on Facebook or Instagram is reported to us as going against local law, but doesn't go against our Community Standards, we may restrict the content's availability in the country where it is alleged to be unlawful."); *About Country Withheld Content*, X Help Center, https://perma.cc/KA26-3HDJ ("[I]f we receive a valid and properly scoped request from an authorized entity, it may be necessary to withhold access to certain content in a particular country from time to time . . . where the content has been found to violate local law(s)."); *Legal Removals*, YouTube, https://perma.cc/8UXG-VLSW ("While our Community Guidelines are

companies—including TikTok—publish reports regarding foreign governments' requests to remove or restrict content based on local laws and the companies' response to those requests.[57]

D. The NSA

21. In a declaration submitted in support of the government's arguments, David Newman, Principal Deputy Assistant Attorney General of the National Security Division of the Department of Justice, states that "[n]othwithstanding . . . extensive negotiations" between the parties, "the Executive Branch was ultimately unable to reach a national security agreement with ByteDance because senior Executive Branch officials concluded that the terms" of that agreement (the "NSA") "would not sufficiently ameliorate th[e] risks" associated with "TikTok's operations in the United States under Chinese ownership."[58] As noted in my first declaration, I am not an expert on the CFIUS process, and I have not undertaken to analyze the CFIUS review in this case.

22. From my perspective, however, none of Mr. Newman's statements alter my assessment that TikTok's draft NSA "provides for a robust system of controls to mitigate data security risks that might arise were foreign governments or adversarial groups . . . to access protected U.S. users data" and that these controls "significantly exceed and improve upon the controls that have been proposed and reportedly implemented by other social media and technology companies, including U.S. companies."[59]

---

policies that apply wherever you are in the world, YouTube is available in more than 100 different countries - so we also have a process in place to comply with local law.").

[57] *See, e.g.*, *Government Removal Requests Report, July 1, 2023 - December 31, 2023*, TikTok (June 6, 2024), https://perma.cc/VR3G-XKDJ; *Content Restrictions Based on Local Law: H2 2023 Report*, Meta, https://perma.cc/TZJ9-U4TP.

[58] Gov't App'x at 46 (Newman Decl.).

[59] Pet'rs App'x at 773 (Weber Decl.).

23. Indeed, several of Mr. Newman's criticisms of the draft NSA are clearly flawed. For example, Mr. Newman states that the NSA's proposal to "anonymize some of the data to which ByteDance would continue to have access" under the NSA would be "insufficient to mitigate the national-security risk[s]" surrounding TikTok because, according to Mr. Newman, "anonymized data is rarely, if ever, truly anonymous."[60] In support of this assertion, Mr. Newman refers to several studies and articles, including a 2019 *New York Times* article, in which anonymized "precise location" data was combined with other publicly available information to "identify, track, and follow" certain individuals.[61] These materials, however, do not establish that TikTok data could be similarly de-anonymized. The evidence the government cites in support of this statement relies on precise GPS location data, but as noted above, current versions of the U.S. TikTok app do not collect the types of "precise geolocation information" used in these studies.[62] Mr. Newman's sources, accordingly, do not establish any deficiency in the NSA relative to anonymization.

24. Mr. Newman also states that the NSA's proposal to have a "Trusted Technology Partner" ("TTP") inspect and monitor source code developed by ByteDance is insufficient to address national security concerns because "a complete review of each line [of code] would be a monumental undertaking," and "perfect review would be an impossibility."[63]

25. The threshold problem with Mr. Newman's statement is his selection of "perfect review" as the yardstick of success. In practice, there is no such thing as "perfect review" of source

---

[60] Gov't App'x at 74 (Newman Decl.).

[61] *Id.* at 74–75 (citing, among other sources, Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://perma.cc/GLQ4-D9MK).

[62] Thompson & Warzel, *supra* note 61.

[63] Gov't App'x at 65.

code. As noted in my first declaration, data security professionals recognize that "data security is not a binary switch that can be toggled on or off."[64] Data security is about trade-offs, and it ultimately is "an exercise in risk management—identifying risks, assessing them, and mitigating those risks to acceptable levels."[65] No organization can assert that its software has no bugs, or that its data security risk has been reduced to zero. Instead, data security professionals seek to mitigate risks to a level such that it is no longer effective or efficient for bad actors to pursue a particular course of action.[66]

26. With respect to data security concerns, as I explained, there are "more effective and efficient means" for a foreign state to "obtain[] relevant information about high-value targets" than attempting to circumvent the types of security protocols outlined in the draft NSA to appropriate TikTok user data.[67] These alternative means include open source intelligence gathering, purchasing data on the open market, and engaging in hacking operations, such as China's reported intrusion of a database maintained by the U.S. Office of Personnel Management—an operation that Mr. Blackburn acknowledges in his declaration.[68] With respect to concerns about content manipulation, foreign states remain able to promote or influence content on other social media platforms, which, unlike TikTok, have not agreed to the types of security and transparency

[64] Pet'rs App'x at 766 (Weber Decl.).

[65] *Id.*

[66] *Id.* at 766–67. As I noted in my first declaration, while "it is virtually impossible to . . . establish that there are no risks associated with a particular application, network, or data storage and management system," TikTok's draft NSA "provides for a robust system of controls to mitigate data security risks that might arise were foreign governments or adversarial groups acting as their agents to attempt to access protected U.S. user data," which "significantly exceed[s] and improve[s] upon the controls that have been proposed and reportedly implemented by other social media and technology companies, including U.S. companies." *Id.* at 766, 773.

[67] *Id.* at 767–69.

[68] *Id.*; *see also* Gov't App'x at 10 (Blackburn Decl.).

protocols described in the NSA. Indeed, as discussed above, these influence operations can be accomplished on other platforms through means as simple as purchasing advertisements on those platforms.[69]

27. By requiring the NSA to enable "perfect review" of TikTok's source code, Mr. Newman is holding TikTok to an impossible standard that is not and could not be applied elsewhere in the technology industry—even with respect to the asserted threat posed by China described in the government's declarations. The government does not require any other technology company, including U.S. technology companies, to be "perfect" in eliminating the risk associated with foreign actors' use of a platform or technology for improper ends. Indeed, the government does not impose this standard on U.S. companies that have Chinese-headquartered subsidiaries and/or engineering operations in China, such as the companies identified in my first declaration.[70] Although many of these companies "face the same theoretical risk" that Chinese employees may interfere with "source code development," the government has not implemented processes and procedures regarding the review of their source code.[71]

28. Setting that issue aside, Mr. Newman does not acknowledge or address industry-standard techniques for effectively assessing data security risk arising from malicious code. From a threat perspective, for example, risk could be substantially mitigated through a prioritized review of proposed changes to the source code, which would be far less burdensome than a review of TikTok's existing source code.[72] Under the NSA, the TTP can review all changes to TikTok's

[69] *See supra* at 12–13.

[70] Pet'rs App'x at 770–71 (Weber Decl.).

[71] *Id.*

[72] Gov't App'x at 65.

source code.[73] Mr. Newman does not explain why this robust approach for source code review of code changes is insufficient to address his concerns.

29. Finally, Mr. Newman cites press reports and ongoing civil court proceedings as support for why "the Executive Branch felt it could not trust ByteDance" to comply with the NSA's provisions, notwithstanding the NSA's requirement that TikTok submit to multiple layers of third-party monitoring in order to verify its compliance with the agreement.[74] Mr. Newman, however, understates the function of third-party monitoring, which is designed to account for a lack of trust. Indeed, the government routinely agrees to third-party monitorships with entities—including Chinese entities—found to have engaged in criminal violations in the national security context.[75] To my knowledge, ByteDance Ltd. and TikTok Inc. have not been found to have engaged in such criminal violations. Mr. Newman does not explain why third-party monitorships are sufficient to address the government's concerns with respect to companies that have been found guilty of criminal offenses but are not sufficient to address its purported concerns with respect to TikTok.

III. Foreign-Owned Media Organizations Operating in the United States

30. Apart from its national security arguments, the government also asserts that TikTok Inc. is differently situated among media and entertainment companies because it is owned by a foreign company and that its activities are accordingly the "speech of a foreigner."[76] In this context as well, the government's statements regarding TikTok are at odds with industry realities. Many news and media organizations in the United States are owned by foreign entities. In terms of news

[73] Pet'rs App'x at 196–97 (NSA Sec. 9.12).

[74] Gov't App'x at 71–73.

[75] *See, e.g.*, Plea Agmt., *United States v. ZTE Corp.*, No. 3:17-cr-00120-K-1 (N.D. Tex. Mar. 7, 2017), ECF No. 3, *available at* https://perma.cc/GNQ8-6HMT.

[76] Gov't Br. at 60.

organizations, *Business Insider* and *Politico* are published by U.S. companies—Insider, Inc. and Politico LLC, respectively—that are owned by the German media company Alex Springer SE.[77] *Fortune* is published by New York-based Fortune Media Corporation, which is owned by Thai businessman Chatchaval Jiaravanon.[78] *Forbes* is owned by a Hong Kong-based investor group.[79] Reuters, which supplies news articles to major U.S. publishers like Gannett and McClatchy, is headquartered in the United Kingdom and owned by a Canadian company.[80] *The Economist*, *The Guardian*, *The Week*, *Mental Floss*, and *Marie Claire* are owned by British companies.[81] *The Spectator* also has British ownership.[82] The *Financial Times* is owned by a Japanese company, and *Al Jazeera* is owned by a Qatari company and funded, in part, by the Government of Qatar.[83]

---

[77] *See* Alyson Shontell, *German Publishing Powerhouse Axel Springer Buys Business Insider at a Whopping $442 Million Valuation*, Business Insider (Sep. 29, 2015), https://perma.cc/U2CE-N5BP; *Axel Springer Completes Acquisition of POLITICO*, Axel Springer (Oct. 19, 2021), https://perma.cc/Z889-BBE2; *Who We Are*, Insider Inc., https://perma.cc/352U-MKYN.

[78] *See* Christine Hauser & Edmund Lee, *Fortune Magazine Sold to Thai Businessman for $150 Million*, N.Y. Times: DealBook (Nov. 9, 2018), https://perma.cc/ATZ4-CAYC; *Fortune Media Corporation*, Fortune (archived Aug. 8, 2020), https://perma.cc/TA37-LC4V.

[79] *See Forbes Media Agrees to Sell Majority Stake to a Group of International Investors to Accelerate the Company's Global Growth*, Forbes (July 18, 2014), https://perma.cc/YW82-U8SS.

[80] *See* David Bauder, *Gannett, McClatchy News Chains Say They Will Stop Using Associated Press Content*, AP (Mar. 19, 2024), https://perma.cc/W2VQ-6Y79.

[81] Jeremy W. Peters, *The Economist Tends to Its Sophisticate Garden*, N.Y. Times (Aug. 8, 2010), https://perma.cc/4DLK-BDL5; *Our Businesses*, The Economist Group, https://perma.cc/VE9N-GZSJ; *About Guardian Media Group*, Guardian, https://perma.cc/T6DG-692Z; Sara Jerde, *Minute Media Acquires Mental Floss*, AdWeek (Sept. 20, 2018), https://perma.cc/WH5A-K7EQ; *About Us*, Minute Media, https://perma.cc/K32W-K89N; *Future Acquires Marie Claire US*, Future plc (May 12, 2021), https://perma.cc/49DK-DR8F; *Our Brands*, Future plc, https://perma.cc/L2TY-K6BD; Future plc, Annual Report FY 2023, at 135, https://perma.cc/MH5J-G8YE.

[82] *Telegraph, Spectator to Not Resume Sale as Barclay Family Repays Debt*, Reuters (Dec. 5, 2023), https://perma.cc/V8CC-39K7.

[83] John Plunkett & Jane Martinson, *Financial Times Sold to Japanese Media Group Nikkei for £844m*, Guardian (July 23, 2015), https://perma.cc/GCU9-N2EK; *Our History 1: Nikkei*

31. Looking beyond news organizations, many other media companies in the United States are owned by foreign entities, including by Chinese companies. Video game developer Riot Games has been owned by the Chinese company Tencent since 2015.[84] Another Chinese company, Wanda Group, owned a controlling share in AMC Theaters from 2012 to 2021.[85] Three of the "Big Five" English-language publishing companies—Hachette Book Group, Macmillan Publishers, and Penguin Random House—are owned by French and German companies.[86] Since the 1990s, Sony Group Corporation, a Japanese company, has owned Sony Pictures Entertainment, one of the "Big Five" American film studios.[87] Two of the "Big Three" record labels in the United States are also foreign owned. Sony Music Entertainment is owned by Sony Group Corporation, a Japanese company, while Universal Music Group is a Dutch-American corporation organized under Dutch law.[88]

Acquires Financial Times(FT), Nikkei (Oct. 1, 2021), https://perma.cc/GRQ6-FGVQ; *About Us*, Al Jazeera, https://perma.cc/4L5S-6Z78.

[84] Allegra Frank, *Riot Games Now Owned Entirely by Tencent*, Polygon (Dec. 16, 2015), https://perma.cc/RW8K-KRYF.

[85] Alex Weprin, *Wanda Sells Off AMC Theatres Stake for $426 Million*, Hollywood Reporter (May 21, 2021), https://perma.cc/3QA9-4K65.

[86] *Bertelsmann Acquires Full Ownership of Penguin Random House*, Bertelsmann (Dec. 18, 2019), https://perma.cc/RF85-9JM3; *Book Publishing*, Hachette Livre, https://perma.cc/6MKW-MFLX; *About Us*, Macmillan Publishers, https://perma.cc/7VXR-J2HJ.

[87] *Affiliated Companies*, Sony, https://perma.cc/MF9J-6GWH.

[88] *Id.*; Caitlin Kelley, *Sony Consolidates Recorded Music and Publishing Under Sony Music Group*, Forbes (July 19, 2019), https://perma.cc/82AP-Z4ZD; *Board and Governance*, Universal Music Group, https://perma.cc/7A6C-DKFL.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 14th day of August, 2024.

Steven Weber

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

TIKTOK INC., and BYTEDANCE LTD., *Petitioners*,	)	
v.	)	No. 24-1113
MERRICK B. GARLAND, in his official Capacity as United States Attorney General, *Respondent*.	)	

DECLARATION OF WILLIAM C. FARRELL

1. I am the Security Officer of TikTok U.S. Data Security Inc. ("TikTok USDS"), which is a wholly owned subsidiary of Petitioner TikTok Inc. In that role, which I have held since May 2022, I lead security, privacy, and compliance functions within TikTok USDS. My focus is working to help ensure that protected U.S. user data is secure, that security controls are in place and effective, and that continuous monitoring and evaluation are conducted to address emerging threats.

I lead a team that includes security researchers, software engineers, network analysts, data scientists, and others dedicated to protecting U.S. user data and preventing unauthorized interference with the U.S. TikTok platform.

2. Between July 2020 and May 2022, I was TikTok's Head of Global Cyber and Data Defense. Before that, I spent 16 years at Booz Allen Hamilton where I led data protection programs, cyber operations, and vulnerability assessments for U.S. government and private-sector clients, including the U.S. Department of Defense and several Fortune 100 companies. My experience includes overseeing efforts to protect sensitive data and communications, supporting the U.S. Department of Defense in both offensive and defensive cyber operations, building world-class cyber-security programs for private sector clients, and helping company boards measure and mitigate cyber risk. I held a Top Secret/Sensitive Compartmented Information clearance. I am a U.S. citizen, born and raised in New York.

3. This declaration responds to certain factual assertions in the government's brief and declarations that relate to my work at TikTok USDS.

4. Since I started working at TikTok in July 2020, I have been deeply involved in the negotiations with the member agencies of the Committee on Foreign Investment in the United States (CFIUS) regarding a potential National Security Agreement (NSA) to resolve the government's concerns that TikTok could pose a risk to U.S. national security.

5. I participated in multiple meetings with and presentations to the CFIUS agencies, including subject matter presentations on protected data, source code, governance, and content moderation mitigations. I also had several additional technical discussions with CFIUS staff of the Department of Justice about the TikTok source code. Throughout this period, I worked closely with our in-house and outside counsel on the technical solutions that were memorialized in that draft Agreement, and received regular updates on the negotiations. I am very familiar with the draft NSA that the company sent to CFIUS on August 23, 2022.

I. NSA Negotiations

6. In his declaration, David Newman describes the August 23, 2022 draft NSA as "ByteDance's final proposal" or the "Final Proposed NSA."[1]

7. By August 23, 2022, we had spent more than a year and a half negotiating the NSA with CFIUS and had exchanged approximately 20 drafts of the Agreement. At the time, we viewed the August 23, 2022 draft as near-final. By then, we had made significant progress in the negotiations, and our focus had shifted to finalizing specific details in the draft Agreement related to, for example, certain definitions, governance provisions, and time periods. Around this time, the Department of Justice began discussing with the company a settlement of the pending litigation and final resolution of the matter.

8. But it was clear that the NSA was still in draft form, and the company was advised by the Departments of the Treasury and Justice that they expected to provide further comments on the draft. The company never received those comments, but was prepared to continue negotiating with the government, including on core terms and the

[1] *See* Gov't App.46; *see also id.* 57-62, 64, 83.

structure of the mitigation solution contemplated by the draft Agreement. The company continued to provide the government updates on the NSA annexes and related materials in fall 2022. Although the company had not received any substantive feedback from the government, the company requested a meeting with the CFIUS Deputies on December 28, 2022. The purpose of this requested meeting was to finalize the NSA, or, if CFIUS were not prepared to finalize the NSA, to hear about any concerns the Committee had so that the company could address them.[2] We formally requested a meeting with the CFIUS Deputies again on February 27, 2023, but that request also was never granted.[3]

II. Insufficiency of Draft NSA

9. Mr. Newman's declaration also identifies several purported flaws in the draft NSA that he claims rendered it insufficient to protect U.S. national security, including that

a. "[S]ignificant volumes of excepted information [would be] able to travel to the PRC for engineering and

[2] App.360.
[3] App.364-65.

commercial reasons," which "would expose U.S. users' data to malign purposes."[4]

b. Anonymization of data is "insufficient to mitigate the national-security risk that the PRC or ByteDance could exploit this data in ways that undermine U.S. national security."[5]

c. The so-called "kill switch" "allowed for a 'temporary stop' only for a specific list of narrowly scoped NSA violations" and would not "give the U.S. Government anything resembling complete discretion" to shut down the platform "based on its own independent assessment of national security risk and assessments from the U.S. Intelligence Community."[6]

10. CFIUS did not raise these three issues during our negotiations as reasons why it viewed the August 23, 2022 draft NSA as inadequate. Had the government communicated their concerns, the

[4] Gov't App.65.
[5] Gov't App.74.
[6] Gov't App.78-79.

company was prepared to discuss modifications to the draft NSA to address them.

11. Mr. Newman's declaration also states that "ByteDance's representations as to the size of the TikTok platform's Source Code leave no doubt that a complete review of each line would be a monumental undertaking. … Even with Oracle's considerable resources, perfect review would be an impossibility."[7]

12. However, as we explained to the Department of Justice, Oracle could prioritize its code review based on the government's (and Oracle's) perceived level of risk and that review could be more targeted and expedited. For example, Oracle could focus first on the code for the user-facing mobile application and leave for later things like open-source code developed by others. Even with these targeted code reviews, we agreed that all code would be available to Oracle, and all code would undergo Oracle analysis using automated tools at Oracle's discretion.

13. The company also recommended supplementing manual source code review with additional reviews by companies with

[7] Gov't App.65.

particular expertise in testing and inspection of mobile apps and platforms. The company explained that such review would be more effective and efficient than line-by-line manual code review. I know from my experience as a government contractor that the methods used by these specialist companies reflect best practices and are relied on by government agencies to identify and address risks or vulnerabilities present in software. In light of these discussions with the government, we engaged HaystackID, OnDefend, and Mandiant as Independent Security Inspectors to provide additional assurance.[8]

III. Protection of U.S. User Data

14. Mr. Newman's declaration also states that the draft NSA "contemplated extensive data flows of U.S. users back to ByteDance and thus to China …."[9]

15. Throughout the draft NSA's negotiations, the company understood that it and the government were aligned that the NSA would limit data flows outside the Oracle cloud as much as possible

[8] "TikTok U.S. Data Security Names Independent Security Inspectors as Part of Digital Integrity and Compliance Journey," TikTok (June 26, 2024), https://perma.cc/L2YE-YEML.
[9] Gov't App.47; *see also id.* at 62, 65.

while allowing the U.S. TikTok platform to continue as part of the global platform. From the very beginning of the NSA negotiations in 2020, our discussions with the government regarding U.S. user data security were premised on distinctions among three different categories of user data: Protected Data, Public Data, and Excepted Data.

16. These distinctions help to ensure that sensitive U.S. user data is adequately protected and that U.S. users can access a TikTok experience that is appropriate, reliable, and integrated with the global platform. While we had extensive discussions with the government about which data should be included in which category, and requested and expected further negotiations on that issue, the government did not object to the *concept* of these three categories of data.

IV. Location of The Recommendation Engine

17. The declarations of Casey Blackburn and David Newman both state that the recommendation algorithm that is used to recommend content to U.S. TikTok users is "stored in" or "resides within" China.[10]

[10] Gov't App.25, 49.

18. The recommendation engine for the U.S. TikTok platform, including the recommendation algorithm, is stored in the Oracle cloud on servers located in the United States. It is subject to the control of TikTok USDS and available for review in its entirety by Oracle.

19. Mr. Newman also states that the company would not agree to "cease collecting U.S. user data or sending it to Beijing to train the algorithm."[11]

20. The recommendation algorithm is trained on U.S. user data in the Oracle cloud by TikTok USDS personnel.

V. TikTok Data Collection

21. The government repeatedly refers to the data collected by TikTok as including a user's "precise location data."[12]

22. The current version of the TikTok app does not collect GPS information from U.S. users. Rather, it collects IP address and country information. This data helps route user data appropriately—for example, routing U.S. user data to the Oracle cloud—and it can render

[11] Gov't App.81-82.
[12] Br. at 1, 18, 27-28; *see also* Gov't App.35-37.

information about a user's *approximate* location, but, unlike GPS, it is an imprecise means of determining a user's location.

23. In his declaration, Kevin Vorndran states that "the TikTok app has access to any data stored in the user's contact list, from names and contact information, to job titles, contact photos, and notes."[13]

24. The TikTok app will, with the user's affirmative permission, access the user's phone contacts and collect information such as names, phone numbers, and email addresses. But that information is automatically "hashed," meaning that it is converted to a unique and anonymized alphanumeric code, before it is sent to the Oracle cloud. In this cloud, the hashed information is used to connect the user with other existing TikTok users, whose information would generate the same hashed value. To the extent the hashed phone contacts are not TikTok users, that information alone cannot be used to recover the original contact information and is deleted. For U.S. users, that hashed information is treated as "protected data" and is not accessible to TikTok or ByteDance employees outside TikTok USDS (subject to exceptions specified by the draft NSA).

[13] Gov't App.35.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this day August 14, 2024.

William C. Farrell

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system on August 15, 2024.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

August 15, 2024

/s/ Alexander A. Berengaut

Alexander A. Berengaut
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
aberengaut@cov.com

Counsel for Petitioners TikTok Inc. and ByteDance Ltd.